

REMARKS

Reconsideration and allowance are respectfully requested in light of the above amendments and the following remarks.

Claims 38-61 have been canceled in favor of new claims 62-97, which recite the subject matter of cancelled claims 1-16 and 18-37, respectively, with revisions to emphasize differences between the claimed invention and the references previously applied in the rejections of claims 1-16 and 18-37. Support for the revisions is provided at least in the specification on page 5, lines 25-29, page 6, lines 19-21, and page 7, line 15.

Claims 38-61 were rejected, under 35 USC §103(a), as being unpatentable over Kaliski (EP 0 807 911) in view of Debry (US 6,314,521). The Applicants respectfully submit that the teachings of Kaliski and Debry have not been applied, and are not applicable, against the subject matter of previous claims 1-16 and 18-37 and the corresponding subject matter defined by new claims 62-97. Accordingly, it is submitted that claims 62-97 are not rendered obvious by the teachings of Kaliski and Debry.

Claims 1-16 and 18-37 were previously rejected for the following reasons. Claims 13-16 and 18-37 were rejected, under 35 USC §102(b), as being anticipated by Sudia et al. (US 6,209,091) (see Final Rejection dated May 26, 2005, section 4). Claims 1-12 were rejected, under 35 USC §103(a), as being

unpatentable over Sudia in view of Schell et al. (US 6,751,735) (see section 6). To the extent these previous rejections may be deemed applicable to new claims 62-97, the Applicants respectfully traverse based on the points set forth below.

It is noted that Sudia describes a multi-step digital signature method and system in which several signing devices participate, using a plurality of private signature key shares, to affix a signature that can be verified using a single public verification key (Sudia abstract). These signing devices are connected to several authorizing agents' trusted devices (col. 6, lines 43-50). The signing devices and trusted devices can be smart cards (col. 6, line 47, and col. 9, line 20).

In Sudia, each signing device and trusted device can store public/ private key pairs (i.e., encryption/decryption keys and signature/verification keys), where the public key of each key pair may be certified by a certification authority. Therefore, each signing device and trusted device can store public key certificates to provide assurance to the public that a public key identified in a certificate is issued by the device whose identification number is in the certificate (col. 1, lines 19-24). These certificates can be signed using Sudia's multi-step method and system (col. 2, lines 25-30).

As Sudia describes in column 8, lines 35-41, and in column 9, lines 45-49, the certificates can also be generated and signed by a manufacturer and then included in a trusted or signing device. These certificates contain the device's serial number and a public key, along with the device's model number and other trusted characteristics. The certificates can also be generated by a temporary administrator. Upon reception of a certification request from a signing or trusted device, an administrator (which is not a PSD) signs with its own private signature key a certificate that comprises the name of the requesting signing device and a public signature verification key generated by the requesting signing device (see col. 10, line 45, through col. 11, line 20, and col. 11, line 53, through col. 12, line 14).

During Sudia's re-certification process, the certificates can also be signed using a multi-step method. Upon reception of a certification request from a signing or trusted device, a plurality of signing devices sign, with their own private signature key shares, a certificate that comprises the name of the requesting signing device and a public signature verification key generated by the requesting signing device (see col. 13, line 53, through col. 14, line 53, and col. 15, line 13, through col. 16, line 3).

In summary, in all the certificate generation methods described by Sudia, a complete certificate is not generated by the requesting signing or trusted device, which generates the public key to be certified. This certificate has to be signed by an authority (manufacturer, temporary administrator, or multiple other signing devices) using a private key of that authority and not a key generated by the requesting signing or trusted device. In particular, this differentiates Sudia from the invention defined by independent claims 62, 86, 90 and 92. The Advisory Action dated September 16, 2005, appears to agree with the discussion above.

However, the Advisory Action suggests that, in Sudia, each (other) signing device has a certificate including a public key and sends its respective public signature verification key and public encryption key certificate back to the lead device (Sudia col. 10, lines 1-27).

To the contrary, the Applicants respectfully submit that Sudia does not teach, in column 10, lines 1-27, that "each signing device generates a complete certificate using public key," as proposed in the Advisory Action (see Advisory Action page 3, lines 2-3).

As also suggested in the Advisory Action, in Sudia, each device also has an electronic key certificate, signed by a

manufacturer, containing a device serial number, a device's public verification key, and a device's public encryption key (see Sudia col. 9, lines 45-49) to verify that the particular key bounded to a particular device is not altered. But it must also be noted, from Sudia's disclosure in column 9, line 40, that the manufacturer has "endowed" each signing device with signature and encryption key pairs, which does not mean that these key pairs are generated by each signing device. Moreover, it is usually not a practice of manufacturers, for cost and efficiency reasons, to generate keys in these signing devices.

Indeed, contrary to a signing device according to Sudia, a PSD according to claim 62 comprises both an asymmetric cryptographic key pair generating algorithm and a key protection certificate generating algorithm, in order to generate both an asymmetric cryptographic key pair and, conditionally with the asymmetric cryptographic key pair generation, a unique digital certificate that comprises a proof of possession by the PSD of both a secret key (shared with the corresponding verification/certification authority) and of the asymmetric cryptographic key pair generated by the PSD. In particular, this makes the methods/systems described in Sudia different from the method/system claimed in independent claims 62, 86, 90 and 92.

Schell describes a data processing system and method for generating or validating a key protection certificate. But, as in Sudia, a certificate must be signed by a certification authority to be valid. Such a certificate is not generated by a PSD whose identifier is contained in the certificate, in dependence of a key generated by the PSD, as in claims 62, 86, 90 and 92.

Accordingly, the Applicants submit that Sudia does not anticipate, and the individual or combined teachings of Sudia and Schell do not suggest, the subject matter defined by claims 62, 86, 90 and 92. Therefore, allowance of claims 62, 86, 90 and 92 and all claims dependent therefrom is warranted.

Moreover, validating a certificate generated by use of one of the methods described in Sudia involves the use, by the verifying system of the public verification key, of the authority that signed the certificate. Therefore, it may need a cross-referencing component for selecting the proper public verification key (and eventually a proper public decryption key) by use of an identifier of the authority. But it does not involve cross-referencing a unique device name of a PSD contained in the certificate with at least one proper cryptographic key and with one proper cryptography algorithm in order to extract useful information from the certificate, as recited in claims 74, 87,

91, and 93. Features of independent claims 74, 87, 91, and 93 concerning a cross-referencing section are thus not disclosed by Sudia.

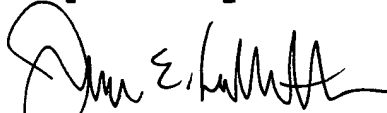
Also, the certificate of claims 74, 87, 91, and 93 will have both encrypted and unencrypted information. The encrypted information is the information that is dependent on a generated cryptographic key. The unencrypted information is the unique device name for the PSD. It is submitted that Sudia does not teach or suggest producing a unique digital certificate that comprises an unencrypted version of a unique device name. With the claimed digital certificate, a device receiving the certificate may extract the unencrypted version of the unique device name to find a match for this name and thereby determine an associated decryption key to use for decrypting the encrypted portion of the certificate. This is not possible with Sudia's system because the unique device name is encrypted. Sudia's receiving device must know which decryption key to use for decrypting the digital certificate without reference to the information within the certificate. Features of independent claims 74, 87, 91 and 93 concerning the cross- referencing are thus not disclosed or suggested by Sudia for this additional reason.

Accordingly, the Applicants respectfully submit that Sudia does not anticipate the subject matter defined by independent claims 74, 87, 91, and 93. Therefore, allowance of claims 74, 87, 91, and 93 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



James E. Ledbetter

Registration No. 28,732

Date: August 1, 2006
JEL/DWW/att

Attorney Docket No. L741.01105
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200